Vlastimil Klíma: Posílený Blue Midnight Wish a druhé kolo soutěže SHA-3,
Crypto-World 12/2009, pp. 4-16, ISSN 1801-2140, 20. prosinec 2009

B. Posílený Blue Midnight Wish a druhé kolo soutěže SHA-3,

Vlastimil Klíma, kryptolog konzultant, Praha
(http://cryptography.hyperlink.cz, v.klima@volny.cz)

Tento článek aktualizuje to, co už jsme o BMW napsali v číslech 3 a 7-8 Crypto-Worldu v letošním roce. Z velké části je tvořen překladem společného příspěvku Gligoroski-Klima na MKB 2009 [3] a několika dalšími aktualizacemi. Záměrně tu zopakujeme věci, které jste už mohli číst, ale děláme to pro pohodlí, abyste si nemuseli brát k ruce další materiály. Výraznou změnou oproti článku v Crypto-Worldu 3/2009 je definice tzv. tweaku, čili úpravy, kterou BMW mohla uplatnit na základě pravidel NISTu pro druhé kolo. Touto změnou jsme výrazně posílili bezpečnost BMW, zejména jako obranu proti tzv. pseudo-útokům (pseudo-kolizím a pseudo-vzorům) a blízkým pseudo-útokům. Tweak je tvořen změnou ve funkcích f_0 a AddElement a přidáním fáze finalizace.

BMW jako rodina

BMW je rodina čtyř hašovacích funkcí (s výstupním kódem 224/256/384/512 bitů), ale lze popsat jako funkce jedna. Funkce BMW224 a BMW384 se vytváří z funkcí BMW256 a BMW512 pouhým zkrácením výstupu a jinou inicializační hodnotou. Funkce BMW256 a BMW512 mají téměř totožný popis, liší se zásadně pouze v délce slova w = 32 bitů nebo w = 64 bitů. Protože operace v BMW jsou zásadně operace se slovy, postačí nám popsat jen variantu BMW256, kterou pro jednoduchost budeme označovat jako BMW.

Iterativní konstrukce

BMW je klasická iterativní hašovací funkce, využívající kompresní funkci. Zpráva, která se má hašovat, se doplní definovaným způsobem tzv. paddingem a počtem zpracovávaných bitů původní zprávy a zarovná se na nejbližší násobek délky bloku 16*w bitů (tj. buď 512 nebo 1024 bitů). Bloky mají tedy 16 slov. Průběžná hašovací hodnota se nastaví na počátku na hodnotu tzv. inicializačního vektoru H(0). Potom se vždy ze staré průběžné hašovací hodnoty a daného bloku zprávy pomocí kompresní funkce vytvoří nová hodnota průběžné haše. Poslední průběžná hodnota haše (nebo její část) je pak prohlášena za skutečnou hodnotu haše. Novinkou u BMW je, že po zpracování posledního bloku doplněné zprávy se provede ještě jedna komprese navíc, tzv. finalizace, viz následující schéma.

1. Předzpracování
(a) Doplň zprávu M jednoznačným definovaným způsobem o délku zprávy v bitech a doplněk
(b) Rozděl zprávu na celistvý násobek (N) m-bitových bloků $M^{(1)}$, ..., $M^{(N)}$.
(c) Nastav počáteční hodnotu průběžné haše $H^{(0)}$ na IV, IV je konstanta.
2. Výpočet haše
For i = 1 to N: $H^{(i)} = f(M^{(i)}, H^{(i-1)})$.
3. Finalizace
$H^{final} = f(H^{(N)}, CONST^{final})$, kde $CONST^{final}$ je konstanta.
4. Závěr
H(M) = dolních n bitů z hodnoty H^{final}.

Obrana proti multiútokům

Aby BMW zabránila Jouxovu útoku, používá průběžnou haš dvakrát tak velkou než je výsledná haš. Nalezení kolize u kompresní funkce má tak složitost $2^{2n/2}$, což je mnohem více než složitost nalezení kolize celé hašovací funkce přímo, což by vyžadovalo jen $2^{n/2}$ výpočtů (pro narozeninový paradox). Průběžnou haš nazýváme dvojitou pumpou (měli bychom říkat

dvojitou rourou, ale v češtině se nám více líbil výraz pumpa, jako „pumpovat“ data). Uvnitř kompresní funkce ve skutečnosti vzniká dokonce čtyřnásobná pumpa Q (bloky Q_a, Q_b) s celkovou šířkou 4n bitů. Nalézat kolize BMW-n prostřednictvím kolize čtyřnásobné pumpy Q je tedy možné pouze nějakým trikem algoritmicky, neboť pravděpodobnostně je to nedosažitelné (pro n = 256/512 bitů je vnitřní šíře Q 1024/2048 bitů). Jedním z důvodů, proč je BMW tak rychlá je, že zpracovává velké bloky zpráv – blok zprávy má m = 2n bitů, takže najednou je zpracováno 512 nebo 1024 bitů.

Označení

V dalším budeme pracovat s proměnnými, které jsou buď slova (w bitů) nebo bloky, které obsahují 16 slov. Takže například M, H, Q_a, Q_b jsou bloky slov (M[0], ..., M[15]), (H[0], ..., H[15]) a Q_a = (Q[0], ..., Q[15]), Q_b = (Q[16], ..., Q[31]). Operace sčítání a odčítání jsou vždy na úrovni slov (tj. modulo 2^w). Na úrovni slov budeme také používat bitové posuny doleva a doprava (shl, shr) nebo rotace doleva (rol), na úrovni bloků pak $ROTL^1(H)$ bude znamenat rotaci slov bloku, tj. $ROTL^1(H)$ = (H[1], ..., H[15], H[0]) a $ROTL^7(H)$ = (H[7], ..., H[5], H[6]). Výrazem rotM označujeme krátce tuto speciální rotaci uvnitř slov bloku M: rotM = ($ROTL^1(M[0])$, $ROTL^2(M[1])$, …, $ROTL^{16}(M[15])$.

Kompresní funkce

Nyní popíšeme kompresní funkci f, zbytek je jasný. Jejím vstupem je stará hodnota průběžné haše H a blok zprávy M, výstupem je nová hodnota průběžné haše newH. Všechno to jsou bloky, obsahující 16 slov. Funkce f je kompozicí funkcí f_0, f_1, f_2, viz obr. 1.

Dekompozice funkce f_0

Funkce f_0 je kompozicí čtyř atomárních transformací které střídají binární (xor) a aritmetické operace (sčítání a odčítání modulo 2^w). Konkrétně máme $Q_a = f_0(H, M) = A_3(A_2(A_1(A_0(H, M)$)), H), kde $X = A_0(H, M) = M \oplus H$ pouze binárně sčítá slova, $W = A_1(X)$ tato slova po pěticích sčítá a odčítá modulo 2^w, načež výsledek prochází přes lineární s-boxy (s_0, s_1, s_2, s_3, s_4), tj. $S = A_2(W)$. Poslední operace je nová (tweak): $Q_a = A_3(S, H) = S + ROTL^1(H)$, kde A_3 sčítá komponenty modulo 2^w. Celá dekompozice je na obr. 3.

Dekompozice funkce f_1

Funkce f_1 má dva vstupy a může být chápána jako slabá bloková šifra $f_1(A, Q_a) = E_A(Q_a)$, u níž je klíč tvořen proměnnou A (AddElement) a otevřený text je Q_a. Výstupem je "šifrový text" Q_b. Tato funkce sice není konstruována jako bloková šifra, ale míchá bity "otevřeného textu (Q_a)" a "klíče (M)" během 16 rund. Je zde také použit princip volitelného parametru pro možné zesílení nebo urychlení hašovací funkce (expandrounds1, počet rund prvního typu). Má dva typy rund, přičemž první je složitější a je standardně použit v prvních dvou rundách. Druhý je jednodušší a je použit ve zbývajících 14 rundách (expandrounds2). Bloková šifra je jednoduchá a lze rozložit na tzv. horní a dolní trojúhelníkové bijekce T^U (upper triangle) a T^L (lower triangle), mezi nimiž je vrstva přičtení klíče K^A (key addition): $f_1 = T^L \bullet K^A \bullet T^U$. Přitom T^U a T^L jsou samy o sobě kombinací binárních a aritmetických kombinací, takže vytváří nelineární blok. Nejprve uvedeme tvorbu klíče. Jeho 16 slov je vidět na obr.2 uprostřed. Symbolicky můžeme zapsat A = AddElement(M, H) = (B(rotM) + K) $\oplus$ $ROTL^7(H)$, kde K je konstanta a funkce B transformuje blok 16 slov rotM nesingulární maticí na blok B(rotM) přičemž vždy sčítá tři slova rotM, viz obr. 5, k výsledku přičte konstantu a na výsledek naxoruje druhý argument. Otevřený text, blok Q_a, je nejprve transformován bez účasti klíče horní trojúhelníkovou (nelineární) transformací $P = T^U(Q_a)$, viz obr. 6, poté se přičte klíč $R = K^A(P, A) = P + A$ a následuje horní trojúhelníková (nelineární) transformace $Q_b = T^L(R)$, viz obr. 7.

Dekompozice funkce f_2

Funkce f_2 používá lineární (binární) bijektivní matici L, která je rozdělena na dvě části L_a a L_b, $L = L_a \oplus L_b$, přičemž i L_a a L_b mají vysokou hodnost (jsou téměř bijektivní), viz obr. 8. Účelem f_2 je komprimovat tři vstupy M, Q_a a Q_b do jednoho výstupu – nové průběžné haše H (newH). Ve funkci hraje velkou úlohu meziproměnná G, která se na H převede jednoduchou bijektivní transformací f_6. Máme $G = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b))$ a $newH = f_6(G) = G + f_5(G)$, viz obr.9. Dílčí výrazy $M \oplus L_a(Q_b)$ a $Q_a \oplus L_b(Q_b)$ označujeme jako $f_3(M, Q_b)$ a $f_4(Q_a, Q_b)$.

Dekompozice kompresní funkce f

Celou složitou funkci f můžeme kupodivu velmi jednoduše zapsat atomárními operacemi velmi jednoduše následovně. Protože ve zkoumání kompresní funkce má velký význam její výstup z hlediska kolizí i hledání vzorů, můžeme místo výstupu $newH = f_6(G)$ zkoumat jeho bijektivní předobraz G. Proto v popisu f můžeme ve většině případů od poslední operace abstrahovat. Máme tak velmi jednoduchý kompaktní zápis f:

$$\mathbf{Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H),}$$
$$\mathbf{Q_b = T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H))),}$$
$$\mathbf{G = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)).}$$

Tab.: Kompaktní zápis kompresní funkce f BMW

BMW aneb Bijections Mounted Widely

Pro návrh BMW bylo důležité, aby použité transformace byly přímo bijekce, pokud měly jeden argument, nebo, v případě dvou argumentů, aby to byly multipermutace, tj. bijekce pokud jeden z argumentů byl fixován. Druhé pravidlo bylo, aby se střídaly transformace binární s operacemi modulo 2^w. O vlastnostech transformací hovoří následující věta.

Věta.

Použité funkce v BMW mají následující vlastnosti.

Funkce f_0:

- $A_0(M, H)$ je multipermutace
- $A_1(X)$ je bijekce
- Všechny s-boxy $s_i(x)$ jsou bijekce
- $A_2(W)$ je bijekce
- $A_3(S, H)$ je multipermutace
- Jestliže H je fixována, $f_0(M, H)$ je bijekce

Funkce f_1:

- $T^U(Q_a)$ je bijekce,
- B(M) je bijekce,
- AddElement(M, H) je multipermutace,
- $K^A(P, A)$ je multipermutace,
- rotM je bijekce,
- $T^L(R)$ je bijekce,
- Když A je fixováno, f_1 je bijekce mezi Q_a a Q_b,
- Když Q_a je fixováno, f_1 je bijekce mezi A a Q_b,

- Když Q_b je fixováno, f_1 je bijekce mezi Q_a a A.

Funkce f_2:

- L je bijekce
- $f_3(M, Q_b)$ je multipermutace,
- $f_4(Q_a, Q_b)$ je multipermutace,
- $f_5(G)$ jako funkce první poloviny G je bijekce,
- $f_6(G)$ je bijekce
- Když Q_b a M jsou fixovány, $f_2(Q_a)$ je bijekce,
- Když Q_b a Q_a jsou fixovány, $f_2(M)$ je bijekce.

Celou kompresní funkci pak můžeme zapsat rovnicemi v tabulce 1, což v podrobném rozlišení je na obr. 2. Pokud si uvědomíme, že těmito operacemi (a žádnými jinými) je zpracován blok zprávy o 512/1024 bitech, je zřejmé, proč je BMW tak rychlá.

Význam multipermutací a bijekcí

Význam je jednoduchý, a to garantovaná změna. Hašovací funkce mají a musí mít problém s kolizemi, a to zejména uvnitř kompresních funkcí. Tím, že BMW používá zásadně bijekce na jednom argumentu nebo když je fixován, tak na druhém argumentu, dociluje toho, že jakákoliv změna se garantovaně propaguje ze vstupu na výstup. Pokud tento princip funguje v celém toku zpracování dat, je změna propagována v celé kompresní funkci. To pochopitelně není možné, protože kompresní funkce musí „komprimovat“ dva bloky (M, H) na jeden blok newH. Protože newH je bijekcí G, můžeme se zabývat jen kompresí (M, H) na G. Komprese je však u BMW dělána až v nejzazším okamžiku, a to poté, co původní vstupy expandujeme na tři bloky – Q_a, Q_b a M. Teprve potom je funkce f_2 komprimuje na jeden blok G. Činí to však jaksi „uvážlivě“, když „ztrácí“ informaci rovnoměrně, neboť f_2 můžeme aproximovat přibližně výrazem $M \oplus L(Q_b) \oplus Q_a$, což je opět multipermutace (M, Q_a, Q_b).

Význam dekompozice

Dekompozice by měla umožnit snadnější analýzu BMW a snadnější důkaz některých vlastností. Konkrétně nám pomohla při vytváření tweaku. Rovnice popisující BMW jsou tak jednoduché, že na nich lze zkoušet mnoho útoků velmi rychle a mnohem jednodušeji než zírat na soustavu rovnic na obrázku 2. Na příkladu ukážeme výhodu dekompozice. Je také velmi výhodné sledovat obrázek 1, kde jsou zakresleny všechny atomární funkce. Atomární je nazýváme proto, že jejich rozklad na menší části je kontraproduktivní nebo nesmyslný a že vyjadřují přesně svůj účel.

Příklad analýzy

Podívejme se na obrázek 1 a řekněme si, že odstraníme složitost vstupu Q_b do G tak, že budeme chtít, aby Q_b bylo konstantní (tj. aby se na Q_b docílila kolize). Potom $G = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)$ bude rovno $G = (M \oplus CONST_a) + (Q_a \oplus CONST_b)$, což při troše nadhledu můžeme považovat za $G = M \oplus Q_a$. Kolizi na G budeme tedy hledat tak, že změny v M se budeme snažit eliminovat změnami v Q_a. Chceme tedy docílit

$Q_b = CONST_1$ a

$M \oplus Q_a = CONST_2$.

Díky dekompozičním rovnicím můžeme tuhle ideu přesně popsat vztahy:

$$T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H))) = CONST_1,$$
$$M \oplus Q_a = CONST_2,$$
$$Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H),$$

nic víc a nic míň.
Z první rovnice můžeme odstranit T^L , protože je to bijekce, takže ji jen „převedeme“ na pravou stranu, kde dostaneme jinou konstantu:

$T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H))) = CONST_3$,
$M \oplus Q_a = CONST_2$,
$Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H)$.

Nyní z těchto rovnic vyloučíme Q_a =, protože manipulovat můžeme dobře jen s H a M. Máme proto

$T^U(A_2(A_1(M \oplus H)) + ROTL^1(H)) + ((B(rotM) + K) \oplus ROTL^7(H))) = CONST_3$,
$M \oplus (A_2(A_1(M \oplus H)) + ROTL^1(H)) = CONST_2$,

Tady máme už vše volitelné, ale také pěkně svázané – dostáváme přesně tolik rovnic kolik je neznámých (ať to vezmeme na bity nebo bloky). Můžeme se pokusit řešit je na úrovni bitů a získat nějaké výhody třeba tím, že ukážeme, že pár bitů (dobré je soustředit se na bity nejnižší nebo nevyšší) některých výrazů nemá nelineární vliv nebo je lze vzájemně vyloučit, čili získat nějaký stupeň volnosti v této příliš přiškrcené soustavě. Pokud se nám to podaří, je to výborné, ale soustavu musíme skutečně dořešit. Takže doufejme, že se Vám to podaří!

Zatím se podíváme, o co se vlastně řešitel této soustavy bude snažit – bude hledat kolizi modifikované kompresní funkce f´, která má šířku 4n bitů! Skutečně, dvě rovnice výše říkají přesně, že hledáme kolizi nebo vzor (nebo pouze pseudokolizi a pseudovzor) funkce $f´(M, H) = (f´_1(M, H), f´_2(M, H))$, kde

$f´_1(M, H) = T^U(A_2(A_1(M \oplus H)) + ROTL^1(H)) + ((B(rotM) + K) \oplus ROTL^7(H))) = CONST_3$,
$f´_2(M, H) = M \oplus (A_2(A_1(M \oplus H)) + ROTL^1(H)) = CONST_2$.

Nepropadáme panice a povšimneme si, že z druhé rovnice můžeme separovat M a H od sebe a přímo vyjádřit vztah mezi M a H:
$M = CONST_2, \oplus (A_2(A_1(M \oplus H)) + ROTL^1(H))$,
který dosadíme do první rovnice:
$T^U(A_2(A_1([CONST_2, \oplus (A_2(A_1(M \oplus H)) + ROTL^1(H))] \oplus H)) + ROTL^1(H)) +$
$((B(rot[CONST_2, \oplus (A_2(A_1(M \oplus H)) + ROTL^1(H))]) + K) \oplus ROTL^7(H))) = CONST_3$.
No a teď už propadnout panice můžeme.
Tohle je rovnice, která přesně vyjadřuje naši ideu. Je s ní ekvivalentní. Pokud ideu chceme použít, musíme umět řešit právě tuto rovnici.

Zkusme tedy druhou ideu – zkusme docílit toho, aby nějakým způsobem byly Q_a i Q_b konstanty.
Máme $Q_a = CONST_1$ a $Q_b = CONST_2$. Výraz G bude pak velmi jednoduchý $G = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)) = (M \oplus CONST_a) + CONST_b$. Protože G je závislé pouze na M, může nám to pomoci při hledání vzoru (pseudovzoru). Stačí splnit rovnice $Q_a = CONST_1$ a $Q_b = CONST_2$.

Máme tedy
$Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H) = CONST_1$

$Q_b = T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H))) = CONST_2$, neboli

$A_2(A_1(M \oplus H)) + ROTL^1(H) = CONST_1$
$T^L(T^U(CONST_1) + ((B(rotM) + K) \oplus ROTL^7(H))) = CONST_2$, neboli

$A_2(A_1(M \oplus H)) + ROTL^1(H) = CONST_1$
$T^L(CONST_3 + ((B(rotM) + K) \oplus ROTL^7(H))) = CONST_2$, neboli

$A_2(A_1(M \oplus H)) + ROTL^1(H) = CONST_1$
$(B(rotM) + K) \oplus ROTL^7(H)) = CONST_4$.

Opět je možné separovat M od H pomocí druhé rovnice:
$H = ROTR^7((B(rotM) + K) \oplus CONST_4)$

a dostáváme pouze první rovnici:
$A_2(A_1(M \oplus [ROTR^7((B(rotM) + K) \oplus CONST_4)])) + ROTL^1([ROTR^7((B(rotM) + K) \oplus CONST_4)]) = CONST_1$

neboli
$A_2(A_1(M \oplus [ROTR^7((B(rotM) + K) \oplus CONST_4)])) + ROTR^6((B(rotM) + K) \oplus CONST_4)) = CONST_1$.

Opět je to čisté vyjádření druhé ideje – takovou rovnici musíme řešit, nic víc, nic míň. Tuto rovnici však musíme umět řešit naprosto přesně, tj. nepomohou nám přibližná řešení. Až ji vyřešíme, čeká nás nemilé překvapení. Získali jsme hodnotu M a nyní dopočítáme hodnotu H = $ROTR^7((B(rotM) + K) \oplus CONST_4)$, nemáme žádný stupeň volnosti. Jenže H, pokud chceme počítat vzor, je pevně daná konstanta (H^{final} nebo H^0) podle toho odkud začínáme útok. Pravděpodobnost, že se do ní strefíme, je však míň než mizivá.

Dostáváme se tak k meritu věci, proč je přidaná finalizační fáze – útočník vždy musí projít minimálně dvě kompresní funkce (jinými slovy musí řešit dvě uvedené soustavy rovnic, kde žádné volné H neexistuje, neboť to jsou konstanty).

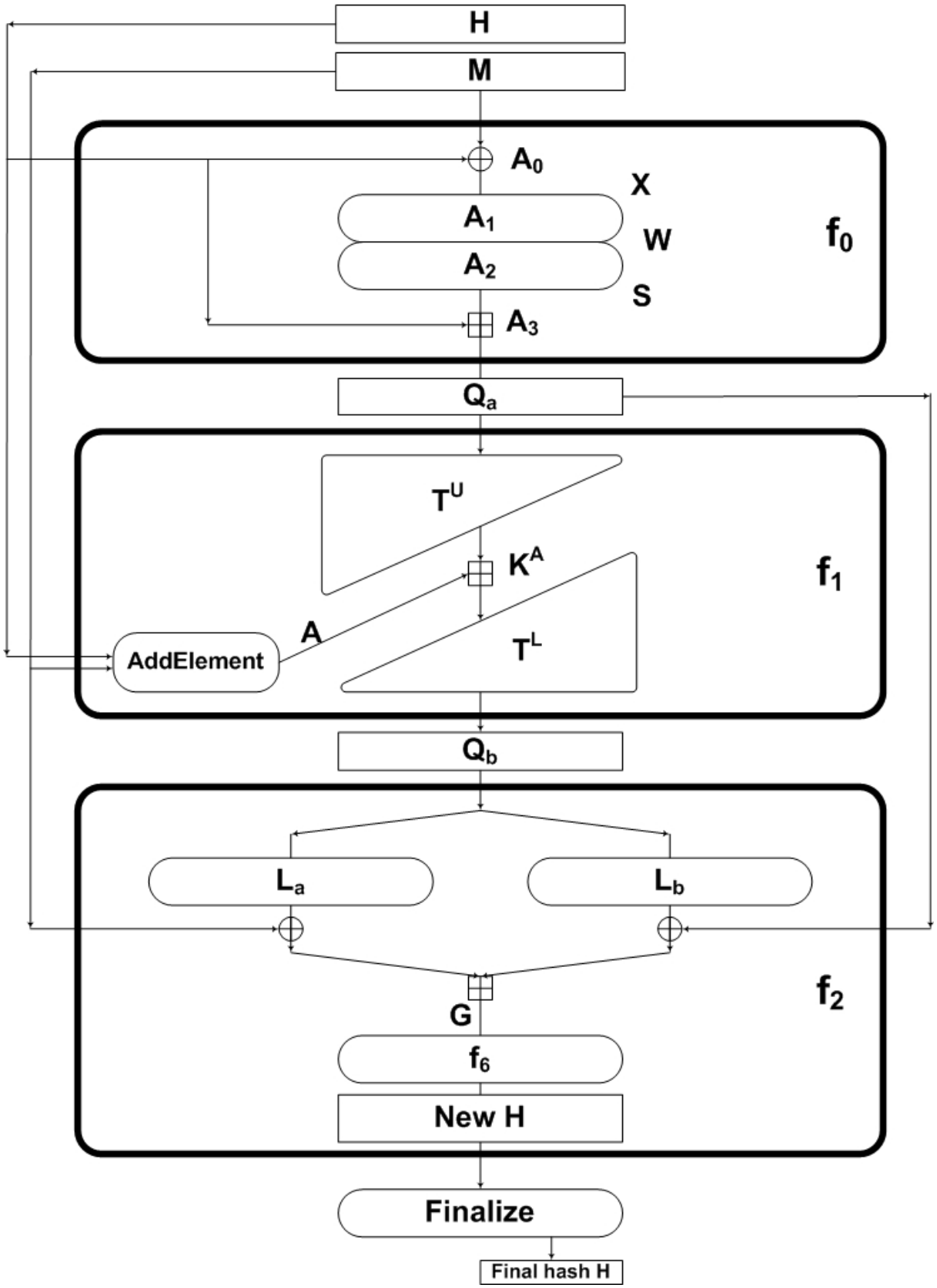
Závěr

V tomto článku jsme uvedli základní popis, úplnou dekompozici a některé vlastnosti hašovací funkce Blue Midnight Wish včetně zesílení (tweak), definované pro druhé kolo soutěže SHA-3. Doufáme, že tento popis podnítí kryptoanalýzu této funkce, která je v současné době nejrychlejším ze 14 kandidátů na SHA-3.

Literatura

[1] stránka NIST k projektu SHA-3: http://csrc.nist.gov/groups/ST/hash/index.html
[2] dokumenty a analýzy BMW a průběžné novinky k projektu SHA-3: http://cryptography.hyperlink.cz/BMW/BMW_CZ.html
[3] Danilo Gligoroski, Vlastimil Klima, On Blue Midnight Wish Decomposition, SantaCrypt 2009, Dec. 3-4, 2009, Prague, Czech Republic, Proceedings of SantaCrypt 2009, ISBN 978-80-904257-0-5, pp. 41-51

Příloha – Obrázky



Obr.1: Kompresní funkce BMW

$$
\begin{array}{lllll}
Q_0 = & H_1 + s_0 (& (M_5 \oplus H_5) - (M_7 \oplus H_7) + (M_{10} \oplus H_{10}) + (M_{13} \oplus H_{13}) + (M_{14} \oplus H_{14}) &) \\
Q_1 = & H_2 + s_1 (& (M_6 \oplus H_6) - (M_8 \oplus H_8) + (M_{11} \oplus H_{11}) + (M_{14} \oplus H_{14}) - (M_{15} \oplus H_{15}) &) \\
Q_2 = & H_3 + s_2 (& (M_0 \oplus H_0) + (M_7 \oplus H_7) + (M_9 \oplus H_9) - (M_{12} \oplus H_{12}) + (M_{15} \oplus H_{15}) &) \\
Q_3 = & H_4 + s_3 (& (M_0 \oplus H_0) - (M_1 \oplus H_1) + (M_8 \oplus H_8) - (M_{10} \oplus H_{10}) + (M_{13} \oplus H_{13}) &) \\
Q_4 = & H_5 + s_4 (& (M_1 \oplus H_1) + (M_2 \oplus H_2) + (M_9 \oplus H_9) - (M_{11} \oplus H_{11}) - (M_{14} \oplus H_{14}) &) \\
Q_5 = & H_6 + s_0 (& (M_3 \oplus H_3) - (M_2 \oplus H_2) + (M_{10} \oplus H_{10}) - (M_{12} \oplus H_{12}) + (M_{15} \oplus H_{15}) &) \\
Q_6 = & H_7 + s_1 (& (M_4 \oplus H_4) - (M_0 \oplus H_0) - (M_3 \oplus H_3) - (M_{11} \oplus H_{11}) + (M_{13} \oplus H_{13}) &) \\
Q_7 = & H_8 + s_2 (& (M_1 \oplus H_1) - (M_4 \oplus H_4) - (M_5 \oplus H_5) - (M_{12} \oplus H_{12}) - (M_{14} \oplus H_{14}) &) \\
Q_8 = & H_9 + s_3 (& (M_2 \oplus H_2) - (M_5 \oplus H_5) - (M_6 \oplus H_6) + (M_{13} \oplus H_{13}) - (M_{15} \oplus H_{15}) &) \\
Q_9 = & H_{10} + s_4 (& (M_0 \oplus H_0) - (M_3 \oplus H_3) + (M_6 \oplus H_6) - (M_7 \oplus H_7) + (M_{14} \oplus H_{14}) &) \\
Q_{10} = & H_{11} + s_0 (& (M_8 \oplus H_8) - (M_1 \oplus H_1) - (M_4 \oplus H_4) - (M_7 \oplus H_7) + (M_{15} \oplus H_{15}) &) \\
Q_{11} = & H_{12} + s_1 (& (M_8 \oplus H_8) - (M_0 \oplus H_0) - (M_2 \oplus H_2) - (M_5 \oplus H_5) + (M_9 \oplus H_9) &) \\
Q_{12} = & H_{13} + s_2 (& (M_1 \oplus H_1) + (M_3 \oplus H_3) - (M_6 \oplus H_6) - (M_9 \oplus H_9) + (M_{10} \oplus H_{10}) &) \\
Q_{13} = & H_{14} + s_3 (& (M_2 \oplus H_2) + (M_4 \oplus H_4) + (M_7 \oplus H_7) + (M_{10} \oplus H_{10}) + (M_{11} \oplus H_{11}) &) \\
Q_{14} = & H_{15} + s_4 (& (M_3 \oplus H_3) - (M_5 \oplus H_5) + (M_8 \oplus H_8) - (M_{11} \oplus H_{11}) - (M_{12} \oplus H_{12}) &) \\
Q_{15} = & H_0 + s_0 (& (M_{12} \oplus H_{12}) - (M_4 \oplus H_4) - (M_6 \oplus H_6) - (M_9 \oplus H_9) + (M_{13} \oplus H_{13}) &)
\end{array}
$$

$$
\begin{aligned}
P_0 &= s1(Q_0) + s2(Q_1) + s3(Q_2) + s0(Q_3) + s1(Q_4) + s2(Q_5) + s3(Q_6) + s0(Q_7) + s1(Q_8) + s2(Q_9) + s3(Q_{10}) + s0(Q_{11}) + s1(Q_{12}) + s2(Q_{13}) + \\
&\quad + s3(Q_{14}) + s0(Q_{15}) \\
P_1 &= s1(Q_1) + s2(Q_2) + s3(Q_3) + s0(Q_4) + s1(Q_5) + s2(Q_6) + s3(Q_7) + s0(Q_8) + s1(Q_9) + s2(Q_{10}) + s3(Q_{11}) + s0(Q_{12}) + s1(Q_{13}) + \\
&\quad + s2(Q_{14}) + s3(Q_{15}) \\
P_2 &= Q_2 + r1(Q_3) + Q_4 + r2(Q_5) + Q_6 + r3(Q_7) + Q_8 + r4(Q_9) + Q_{10} + r5(Q_{11}) + Q_{12} + r6(Q_{13}) + Q_{14} + r7(Q_{15}) \\
P_3 &= Q_3 + r1(Q_4) + Q_5 + r2(Q_6) + Q_7 + r3(Q_8) + Q_9 + r4(Q_{10}) + Q_{11} + r5(Q_{12}) + Q_{13} + r6(Q_{14}) + Q_{15} \\
P_4 &= Q_4 + r1(Q_5) + Q_6 + r2(Q_7) + Q_8 + r3(Q_9) + Q_{10} + r4(Q_{11}) + Q_{12} + r5(Q_{13}) + Q_{14} + r6(Q_{15}) \\
P_5 &= Q_5 + r1(Q_6) + Q_7 + r2(Q_8) + Q_9 + r3(Q_{10}) + Q_{11} + r4(Q_{12}) + Q_{13} + r5(Q_{14}) + Q_{15} \\
P_6 &= Q_6 + r1(Q_7) + Q_8 + r2(Q_9) + Q_{10} + r3(Q_{11}) + Q_{12} + r4(Q_{13}) + Q_{14} + r5(Q_{15}) \\
P_7 &= Q_7 + r1(Q_8) + Q_9 + r2(Q_{10}) + Q_{11} + r3(Q_{12}) + Q_{13} + r4(Q_{14}) + Q_{15} \\
P_8 &= Q_8 + r1(Q_9) + Q_{10} + r2(Q_{11}) + Q_{12} + r3(Q_{13}) + Q_{14} + r4(Q_{15}) \\
P_9 &= Q_9 + r1(Q_{10}) + Q_{11} + r2(Q_{12}) + Q_{13} + r3(Q_{14}) + Q_{15} \\
P_{10} &= Q_{10} + r1(Q_{11}) + Q_{12} + r2(Q_{13}) + Q_{14} + r3(Q_{15}) \\
P_{11} &= Q_{11} + r1(Q_{12}) + Q_{13} + r2(Q_{14}) + Q_{15} \\
P_{12} &= Q_{12} + r1(Q_{13}) + Q_{14} + r2(Q_{15}) \\
P_{13} &= Q_{13} + r1(Q_{14}) + Q_{15} \\
P_{14} &= Q_{14} + r1(Q_{15}) \\
P_{15} &= Q_{15}
\end{aligned}
$$

$$
\begin{array}{lllllllllll}
R_0 = & P_0 + A_0 & = & P_0 + (& H_6 \oplus (& ROTL^1(M_0) + & ROTL^4(M_3) - & ROTL^{11}(M_{10}) + & K_0)) \\
R_1 = & P_1 + A_1 & = & P_1 + (& H_7 \oplus (& ROTL^2(M_1) + & ROTL^5(M_4) - & ROTL^{12}(M_{11}) + & K_1)) \\
R_2 = & P_2 + A_2 & = & P_2 + (& H_8 \oplus (& ROTL^3(M_2) + & ROTL^6(M_5) - & ROTL^{13}(M_{12}) + & K_2)) \\
R_3 = & P_3 + A_3 & = & P_3 + (& H_9 \oplus (& ROTL^4(M_3) + & ROTL^7(M_6) - & ROTL^{14}(M_{13}) + & K_3)) \\
R_4 = & P_4 + A_4 & = & P_4 + (& H_{10} \oplus (& ROTL^5(M_4) + & ROTL^8(M_7) - & ROTL^{15}(M_{14}) + & K_4)) \\
R_5 = & P_5 + A_5 & = & P_5 + (& H_{11} \oplus (& ROTL^6(M_5) + & ROTL^9(M_8) - & ROTL^{16}(M_{15}) + & K_5)) \\
R_6 = & P_6 + A_6 & = & P_6 + (& H_{12} \oplus (& ROTL^7(M_6) + & ROTL^{10}(M_9) - & ROTL^1(M_0) + & K_6)) \\
R_7 = & P_7 + A_7 & = & P_7 + (& H_{13} \oplus (& ROTL^8(M_7) + & ROTL^{11}(M_{10}) - & ROTL^2(M_1) + & K_7)) \\
R_8 = & P_8 + A_8 & = & P_8 + (& H_{14} \oplus (& ROTL^9(M_8) + & ROTL^{12}(M_{11}) - & ROTL^3(M_2) + & K_8)) \\
R_9 = & P_9 + A_8 & = & P_9 + (& H_{15} \oplus (& ROTL^{10}(M_9) + & ROTL^{13}(M_{12}) - & ROTL^4(M_3) + & K_9)) \\
R_{10} = & P_{10} + A_{10} & = & P_{10} + (& H_0 \oplus (& ROTL^{11}(M_{10}) + & ROTL^{14}(M_{13}) - & ROTL^5(M_4) + & K_{10})) \\
R_{11} = & P_{11} + A_{11} & = & P_{11} + (& H_1 \oplus (& ROTL^{12}(M_{11}) + & ROTL^{15}(M_{14}) - & ROTL^6(M_5) + & K_{11})) \\
R_{12} = & P_{12} + A_{12} & = & P_{12} + (& H_2 \oplus (& ROTL^{13}(M_{12}) + & ROTL^{16}(M_{15}) - & ROTL^7(M_6) + & K_{12})) \\
R_{13} = & P_{13} + A_{13} & = & P_{13} + (& H_3 \oplus (& ROTL^{14}(M_{13}) + & ROTL^1(M_0) - & ROTL^8(M_7) + & K_{13})) \\
R_{14} = & P_{14} + A_{14} & = & P_{14} + (& H_4 \oplus (& ROTL^{15}(M_{14}) + & ROTL^2(M_1) - & ROTL^9(M_8) + & K_{14})) \\
R_{15} = & P_{15} + A_{15} & = & P_{15} + (& H_5 \oplus (& ROTL^{16}(M_{15}) + & ROTL^3(M_2) - & ROTL^{10}(M_9) + & K_{15}))
\end{array}
$$

$$
\begin{aligned}
Q_{16} &= R_0 \\
Q_{17} &= R_1 + s0(Q_{16}) \\
Q_{18} &= R_2 + s4(Q_{16}) + s5(Q_{17}) \\
Q_{19} &= R_3 + r7(Q_{16}) + s4(Q_{17}) + s5(Q_{18}) \\
Q_{20} &= R_4 + Q_{16} + r7(Q_{17}) + s4(Q_{18}) + s5(Q_{19}) \\
Q_{21} &= R_5 + r6(Q_{16}) + Q_{17} + r7(Q_{18}) + s4(Q_{19}) + s5(Q_{20}) \\
Q_{22} &= R_6 + Q_{16} + r6(Q_{17}) + Q_{18} + r7(Q_{19}) + s4(Q_{20}) + s5(Q_{21}) \\
Q_{23} &= R_7 + r5(Q_{16}) + Q_{17} + r6(Q_{18}) + Q_{19} + r7(Q_{20}) + s4(Q_{21}) + s5(Q_{22}) \\
Q_{24} &= R_8 + Q_{16} + r5(Q_{17}) + Q_{18} + r6(Q_{19}) + Q_{20} + r7(Q_{21}) + s4(Q_{22}) + s5(Q_{23}) \\
Q_{25} &= R_9 + r4(Q_{16}) + Q_{17} + r5(Q_{18}) + Q_{19} + r6(Q_{20}) + Q_{21} + r7(Q_{22}) + s4(Q_{23}) + s5(Q_{24}) \\
Q_{26} &= R_{10} + Q_{16} + r4(Q_{17}) + Q_{18} + r5(Q_{19}) + Q_{20} + r6(Q_{21}) + Q_{22} + r7(Q_{23}) + s4(Q_{24}) + s5(Q_{25}) \\
Q_{27} &= R_{11} + r3(Q_{16}) + Q_{17} + r4(Q_{18}) + Q_{19} + r5(Q_{20}) + Q_{21} + r6(Q_{22}) + Q_{23} + r7(Q_{24}) + s4(Q_{25}) + s5(Q_{26}) \\
Q_{28} &= R_{12} + Q_{16} + r3(Q_{17}) + Q_{18} + r4(Q_{19}) + Q_{20} + r5(Q_{21}) + Q_{22} + r6(Q_{23}) + Q_{24} + r7(Q_{25}) + s4(Q_{26}) + s5(Q_{27}) \\
Q_{29} &= R_{13} + r2(Q_{16}) + Q_{17} + r3(Q_{18}) + Q_{19} + r4(Q_{20}) + Q_{21} + r5(Q_{22}) + Q_{23} + r6(Q_{24}) + Q_{25} + r7(Q_{26}) + s4(Q_{27}) + s5(Q_{28}) \\
Q_{30} &= R_{14} + Q_{16} + r2(Q_{17}) + Q_{18} + r3(Q_{19}) + Q_{20} + r4(Q_{21}) + Q_{22} + r5(Q_{23}) + Q_{24} + r6(Q_{25}) + Q_{26} + r7(Q_{27}) + s4(Q_{28}) + s5(Q_{29}) \\
Q_{31} &= R_{15} + r1(Q_{16}) + Q_{17} + r2(Q_{18}) + Q_{19} + r3(Q_{20}) + Q_{21} + r4(Q_{22}) + Q_{23} + r5(Q_{24}) + Q_{25} + r6(Q_{26}) + Q_{27} + r7(Q_{28}) + s4(Q_{29}) + s5(Q_{30})
\end{aligned}
$$

$$
\begin{array}{lllll}
H_0 = & & (SHL^5(XH) \oplus SHR^5(Q_{16}) \oplus M_0) + & (XL \oplus Q_{24} \oplus Q_0) \\
H_1 = & & (SHR^7(XH) \oplus SHL^8(Q_{17}) \oplus M_1) + & (XL \oplus Q_{25} \oplus Q_1) \\
H_2 = & & (SHR^5(XH) \oplus SHL^5(Q_{18}) \oplus M_2) + & (XL \oplus Q_{26} \oplus Q_2) \\
H_3 = & & (SHR^1(XH) \oplus SHL^5(Q_{19}) \oplus M_3) + & (XL \oplus Q_{27} \oplus Q_3) \\
H_4 = & & (SHR^3(XH) \oplus Q_{20} \oplus M_4) + & (XL \oplus Q_{28} \oplus Q_4) \\
H_5 = & & (SHL^6(XH) \oplus SHR^6(Q_{21}) \oplus M_5) + & (XL \oplus Q_{29} \oplus Q_5) \\
H_6 = & & (SHR^4(XH) \oplus SHL^6(Q_{22}) \oplus M_6) + & (XL \oplus Q_{30} \oplus Q_6) \\
H_7 = & & (SHR^{11}(XH) \oplus SHL^2(Q_{23}) \oplus M_7) + & (XL \oplus Q_{31} \oplus Q_7) \\
H_8 = & ROTL^9(H_4) + & (XH \oplus Q_{24} \oplus M_8) + & (SHL^8(XL) \oplus Q_{23} \oplus Q_8) \\
H_9 = & ROTL^{10}(H_5) + & (XH \oplus Q_{25} \oplus M_9) + & (SHR^6(XL) \oplus Q_{16} \oplus Q_9) \\
H_{10} = & ROTL^{11}(H_6) + & (XH \oplus Q_{26} \oplus M_{10}) + & (SHL^6(XL) \oplus Q_{17} \oplus Q_{10}) \\
H_{11} = & ROTL^{12}(H_7) + & (XH \oplus Q_{27} \oplus M_{11}) + & (SHL^4(XL) \oplus Q_{18} \oplus Q_{11}) \\
H_{12} = & ROTL^{13}(H_0) + & (XH \oplus Q_{28} \oplus M_{12}) + & (SHR^3(XL) \oplus Q_{19} \oplus Q_{12}) \\
H_{13} = & ROTL^{14}(H_1) + & (XH \oplus Q_{29} \oplus M_{13}) + & (SHR^4(XL) \oplus Q_{20} \oplus Q_{13}) \\
H_{14} = & ROTL^{15}(H_2) + & (XH \oplus Q_{30} \oplus M_{14}) + & (SHR^7(XL) \oplus Q_{21} \oplus Q_{14}) \\
H_{15} = & ROTL^{16}(H_3) + & (XH \oplus Q_{31} \oplus M_{15}) + & (SHR^2(XL) \oplus Q_{22} \oplus Q_{15})
\end{array}
$$

Obr.2: Kompletní popis kompresní funkce rovnicemi

$W = A_1(X)$:

$$
\begin{array}{lcl}
W_0 &=& X_5 - X_7 + X_{10} + X_{13} + X_{14} \\
W_1 &=& X_6 - X_8 + X_{11} + X_{14} - X_{15} \\
W_2 &=& X_0 + X_7 + X_9 - X_{12} + X_{15} \\
W_3 &=& X_0 - X_1 + X_8 - X_{10} + X_{13} \\
W_4 &=& X_1 + X_2 + X_9 - X_{11} - X_{14} \\
W_5 &=& X_3 - X_2 + X_{10} - X_{12} + X_{15} \\
W_6 &=& X_4 - X_0 - X_3 - X_{11} + X_{13} \\
W_7 &=& X_1 - X_4 - X_5 - X_{12} - X_{14} \\
W_8 &=& X_2 - X_5 - X_6 + X_{13} - X_{15} \\
W_9 &=& X_0 - X_3 + X_6 - X_7 + X_{14} \\
W_{10} &=& X_8 - X_1 - X_4 - X_7 + X_{15} \\
W_{11} &=& X_8 - X_0 - X_2 - X_5 + X_9 \\
W_{12} &=& X_1 + X_3 - X_6 - X_9 + X_{10} \\
W_{13} &=& X_2 + X_4 + X_7 + X_{10} + X_{11} \\
W_{14} &=& X_3 - X_5 + X_8 - X_{11} - X_{12} \\
W_{15} &=& X_{12} - X_4 - X_6 - X_9 + X_{13}
\end{array}
$$

$S = A_2(W)$:

$$
\begin{array}{llll}
S_0 = s_0(W_0) & S_1 = s_1(W_1) & S_2 = s_2(W_2) & S_3 = s_3(W_3) \\
S_4 = s_4(W_4) & S_5 = s_0(W_5) & S_6 = s_1(W_6) & S_7 = s_2(W_7) \\
S_8 = s_3(W_8) & S_9 = s_4(W_9) & S_{10} = s_0(W_{10}) & S_{11} = s_1(W_{11}) \\
S_{12} = s_2(W_{12}) & S_{13} = s_3(W_{13}) & S_{14} = s_4(W_{14}) & S_{15} = s_0(W_{15})
\end{array}
$$

$Q_a = A_3(S, H)$:

$$
\begin{array}{llll}
Q_0 = S_0 + H_1; & Q_1 = S_1 + H_2; & Q_2 = S_2 + H_3; & Q_3 = S_3 + H_4; \\
Q_4 = S_4 + H_5; & Q_5 = S_5 + H_6; & Q_6 = S_6 + H_7; & Q_7 = S_7 + H_8; \\
Q_8 = S_8 + H_9; & Q_9 = S_9 + H_{10}; & Q_{10} = S_{10} + H_{11}; & Q_{11} = S_{11} + H_{12}; \\
Q_{12} = S_{12} + H_{13}; & Q_{13} = S_{13} + H_{14}; & Q_{14} = S_{14} + H_{15}; & Q_{15} = S_{15} + H_0;
\end{array}
$$

Obr.3: Dekompozice funkce f_0

$$
\begin{array}{l}
s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{19}(x) \\
s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^8(x) \oplus ROTL^{23}(x) \\
s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{12}(x) \oplus ROTL^{25}(x) \\
s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{15}(x) \oplus ROTL^{29}(x) \\
s_4(x) = SHR^1(x) \oplus x \\
s_5(x) = SHR^2(x) \oplus x \\
r_1(x) = ROTL^3(x) \\
r_2(x) = ROTL^7(x) \\
r_3(x) = ROTL^{13}(x) \\
r_4(x) = ROTL^{16}(x) \\
r_5(x) = ROTL^{19}(x) \\
r_6(x) = ROTL^{23}(x) \\
r_7(x) = ROTL^{27}(x)
\end{array}
$$

Obr.4: Používané lineární s-boxy a rotace

$$
\begin{aligned}
D_0 &= M_0 + M_3 - M_{10} \\
D_1 &= M_1 + M_4 - M_{11} \\
D_2 &= M_2 + M_5 - M_{12} \\
D_3 &= M_3 + M_6 - M_{13} \\
D_4 &= M_4 + M_7 - M_{14} \\
D_5 &= M_5 + M_8 - M_{15} \\
D_6 &= M_6 + M_9 - M_0 \\
D_7 &= M_7 + M_{10} - M_1 \\
D_8 &= M_8 + M_{11} - M_2 \\
D_9 &= M_9 + M_{12} - M_3 \\
D_{10} &= M_{10} + M_{13} - M_4 \\
D_{11} &= M_{11} + M_{14} - M_5 \\
D_{12} &= M_{12} + M_{15} - M_6 \\
D_{13} &= M_{13} + M_0 - M_7 \\
D_{14} &= M_{14} + M_1 - M_8 \\
D_{15} &= M_{15} + M_2 - M_9
\end{aligned}
$$

Obr.5: Funkce B(M)

```
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
P[ 0] =
s1(Q[ 0])+s2(Q[ 1])+s3(Q[ 2])+s0(Q[ 3])+s1(Q[ 4])+s2(Q[ 5])+s3(Q[ 6])+
s0(Q[ 7])+s1(Q[ 8])+s2(Q[ 9])+s3(Q[10])+s0(Q[11])+s1(Q[12])+s2(Q[13])+
s3(Q[14])+s0(Q[15])

P[ 1]=
s1(Q[ 1])+s2(Q[ 2])+s3(Q[ 3])+s0(Q[ 4])+s1(Q[ 5])+s2(Q[ 6])+s3(Q[ 7])+
s0(Q[ 8])+s1(Q[ 9])+s2(Q[10])+s3(Q[11])+s0(Q[12])+s1(Q[13])+s2(Q[14])+
s3(Q[15])

P[02]=
Q[ 2]+r1(Q[ 3])+Q[ 4]+r2(Q[ 5])+Q[ 6]+r3(Q[ 7])+Q[ 8]+r4(Q[ 9])+
Q[10]+r5(Q[11])+Q[12]+r6(Q[13])+Q[14]+r7(Q[15])

P[03]=
Q[ 3]+r1(Q[ 4])+Q[ 5]+r2(Q[ 6])+Q[ 7]+r3(Q[ 8])+Q[ 9]+r4(Q[10])+
Q[11]+r5(Q[12])+Q[13]+r6(Q[14])+Q[15]

P[ 4]=
Q[ 4]+r1(Q[ 5])+Q[ 6]+r2(Q[ 7])+Q[ 8]+r3(Q[ 9])+Q[10]+r4(Q[11])+
Q[12]+r5(Q[13])+Q[14]+r6(Q[15])

P[ 5]=
Q[ 5]+r1(Q[ 6])+Q[ 7]+r2(Q[ 8])+Q[ 9]+r3(Q[10])+Q[11]+r4(Q[12)+
Q[13]+r5(Q[14])+Q[15]

P[ 6]=
Q[ 6]+r1(Q[ 7])+Q[ 8]+r2(Q[ 9])+Q[10]+r3(Q[11])+Q[12]+r4(Q[13])+
Q[14]+r5(Q[15])

P[ 7]=
Q[ 7]+r1(Q[ 8])+Q[ 9]+r2(Q[10])+Q[11]+r3(Q[12])+Q[13]+r4(Q[14])+
Q[15]

P[ 8]=
Q[ 8]+r1(Q[ 9])+Q[10]+r2(Q[11])+Q[12]+r3(Q[13])+Q[14]+r4(Q[15])
```

```
P[ 9]=
Q[ 9]+r1(Q[10])+Q[11]+r2(Q[12])+Q[13]+r3(Q[14])+Q[15]

P[10]=
Q[10]+r1(Q[11])+Q[12]+r2(Q[13])+Q[14]+r3(Q[15])

P[11]=
Q[11]+r1(Q[12])+Q[13]+r2(Q[14])+Q[15]

P[12]=
Q[12]+r1(Q[13])+Q[14]+r2(Q[15])

P[13]=
Q[13]+r1(Q[14])+Q[15]

P[14]=
Q[14]+r1(Q[15])

P[15]=
Q[15]
```

Obr. 6: Horní trojúhelníková transformace P = (P[0], ..., P[15]) = $T^U(Q_a)$ = T^U(Q[0], ..., Q[15])

```
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Q[16]=
R[0]

Q[17]=
R[1] + s0(Q[16])

Q[18]=
R[2] +s4(Q[16])+s5(Q[17])

Q[19]=
R[3] +r7(Q[16])+s4(Q[17])+s5(Q[18])

Q[20]=
R[4] +Q[16]+r7(Q[17])+s4(Q[18])+s5(Q[19])

Q[21]=
R[5] +r6(Q[16])+Q[17]+r7(Q[18])+s4(Q[19])+s5(Q[20])

Q[22]=
R[6] +Q[16]+r6(Q[17])+Q[18]+r7(Q[19])+s4(Q[20])+s5(Q[21])

Q[23]=
R[7] +r5(Q[16])+Q[17]+r6(Q[18])+Q[19]+r7(Q[20])+s4(Q[21])+s5(Q[22])

Q[24]=
R[8]+
Q[16]+r5(Q[17])+Q[18]+r6(Q[19])+Q[20]+r7(Q[21])+s4(Q[22])+s5(Q[23])

Q[25]=
R[9]+r4(Q[16])+Q[17]+r5(Q[18])+Q[19]+r6(Q[20])+Q[21]+r7(Q[22])+s4(Q[23])+s5
(Q[24])

Q[26]=
```

```
R[10]+Q[16]+r4(Q[17])+Q[18]+r5(Q[19])+Q[20]+r6(Q[21])+Q[22]+r7(Q[23])+s4(Q[
24])+s5(Q[25])

Q[27]=
R[11]+r3(Q[16])+Q[17]+r4(Q[18])+Q[19]+r5(Q[20])+Q[21]+r6(Q[22])+Q[23]+r7(Q[
24])+s4(Q[25])+s5(Q[26])

Q[28]=
R[12]+Q[16]+r3(Q[17])+Q[18]+r4(Q[19])+Q[20]+r5(Q[21])+Q[22]+r6(Q[23])+Q[24]
+r7(Q[25])+s4(Q[26])+s5(Q[27])

Q[29]=
R[13]+r2(Q[16])+Q[17]+r3(Q[18])+Q[19]+r4(Q[20])+Q[21]+r5(Q[22])+Q[23]+r6(Q[
24])+Q[25]+r7(Q[26])+s4(Q[27])+s5(Q[28])

Q[30]=
R[14]+Q[16]+r2(Q[17])+Q[18]+r3(Q[19])+Q[20]+r4(Q[21])+Q[22]+r5(Q[23])+Q[24]
+r6(Q[25])+Q[26]+r7(Q[27])+s4(Q[28])+s5(Q[29])

Q[31]=
R[15]+r1(Q[16])+Q[17]+r2(Q[18])+Q[19]+r3(Q[20])+Q[21]+r4(Q[22])+Q[23]+r5(Q[
24])+Q[25]+r6(Q[26])+Q[27]+r7(Q[28])+s4(Q[29])+s5(Q[30])
```

Obr. 7: Dolní trojúhelníková transformace $QB_b = T^L(R) = (Q[16], ..., Q[31])$.
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

$$L_a(Qb) = \begin{pmatrix} SHL^5(XH) \oplus & SHR^5(Q_{16}^{(i)}) \\ SHR^7(XH) \oplus & SHL^8(Q_{17}^{(i)}) \\ SHR^5(XH) \oplus & SHL^5(Q_{18}^{(i)}) \\ SHR^1(XH) \oplus & SHL^5(Q_{19}^{(i)}) \\ SHR^3(XH) \oplus & Q_{20}^{(i)} \\ SHL^6(XH) \oplus & SHR^6(Q_{21}^{(i)}) \\ SHR^4(XH) \oplus & SHL^6(Q_{22}^{(i)}) \\ SHR^{11}(XH) \oplus & SHL^2(Q_{23}^{(i)}) \\ XH \oplus & Q_{24}^{(i)} \\ XH \oplus & Q_{25}^{(i)} \\ XH \oplus & Q_{26}^{(i)} \\ XH \oplus & Q_{27}^{(i)} \\ XH \oplus & Q_{28}^{(i)} \\ XH \oplus & Q_{29}^{(i)} \\ XH \oplus & Q_{30}^{(i)} \\ XH \oplus & Q_{31}^{(i)} \end{pmatrix} \quad L_b(Qb) = \begin{pmatrix} XL \oplus & Q_{24}^{(i)} \\ XL \oplus & Q_{25}^{(i)} \\ XL \oplus & Q_{26}^{(i)} \\ XL \oplus & Q_{27}^{(i)} \\ XL \oplus & Q_{28}^{(i)} \\ XL \oplus & Q_{29}^{(i)} \\ XL \oplus & Q_{30}^{(i)} \\ XL \oplus & Q_{31}^{(i)} \\ SHL^8(XL) \oplus & Q_{23}^{(i)} \\ SHR^6(XL) \oplus & Q_{16}^{(i)} \\ SHL^6(XL) \oplus & Q_{17}^{(i)} \\ SHL^4(XL) \oplus & Q_{18}^{(i)} \\ SHR^3(XL) \oplus & Q_{19}^{(i)} \\ SHR^4(XL) \oplus & Q_{20}^{(i)} \\ SHR^7(XL) \oplus & Q_{21}^{(i)} \\ SHR^2(XL) \oplus & Q_{22}^{(i)} \end{pmatrix}$$

Obr.8: Dvě části bijekceL, $L = L_a \oplus L_b$

$$f_5(X) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ ROTL^{9}(X_4) \\ ROTL^{10}(X_5) \\ ROTL^{11}(X_6) \\ ROTL^{12}(X_7) \\ ROTL^{13}(X_0) \\ ROTL^{14}(X_1) \\ ROTL^{15}(X_2) \\ ROTL^{16}(X_3) \end{pmatrix}$$

Obr.9: Funkce f5